



A MITEL  
PRODUCT  
GUIDE

# MiContact Center Enterprise

## Configure MBG for WEBRTC - Operating Instructions

**Release 9.8**  
Document Version 1.0

August 2025



## Notices

The information contained in this document is believed to be accurate in all respects but is not warranted by **Mitel Networks™ Corporation (MITEL®)**. The

information is

subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes. No part of this document can be reproduced or transmitted in any form or by any means - electronic or mechanical - for any purpose without written permission from Mitel Networks Corporation.

## Trademarks

The trademarks, service marks, logos and graphics (collectively "Trademarks") appearing on Mitel's Internet sites or in its publications are registered and unregistered trademarks of Mitel Networks Corporation (MNC) or its subsidiaries (collectively "Mitel") or others. Use of the Trademarks is prohibited without the express consent from Mitel. Please contact our legal department at [legal@mitel.com](mailto:legal@mitel.com) for additional information. For a list of the worldwide Mitel Networks Corporation registered trademarks, please refer to the website:

<http://www.mitel.com/trademarks>.

®,™ Trademark of Mitel Networks Corporation

© Copyright 2025, Mitel Networks Corporation All rights reserved

# INTRODUCTION

The Web Agent application contains WebRTC components so that it can be used as a WebRTC powered soft phone for voice calls. This requires that a Mitel Border Gateway (MBG) to be configured as a WebRTC Gateway connected to the MX-ONE call manager. It is highly recommended that the technician configuring the MBG system is trained and certified on that product.

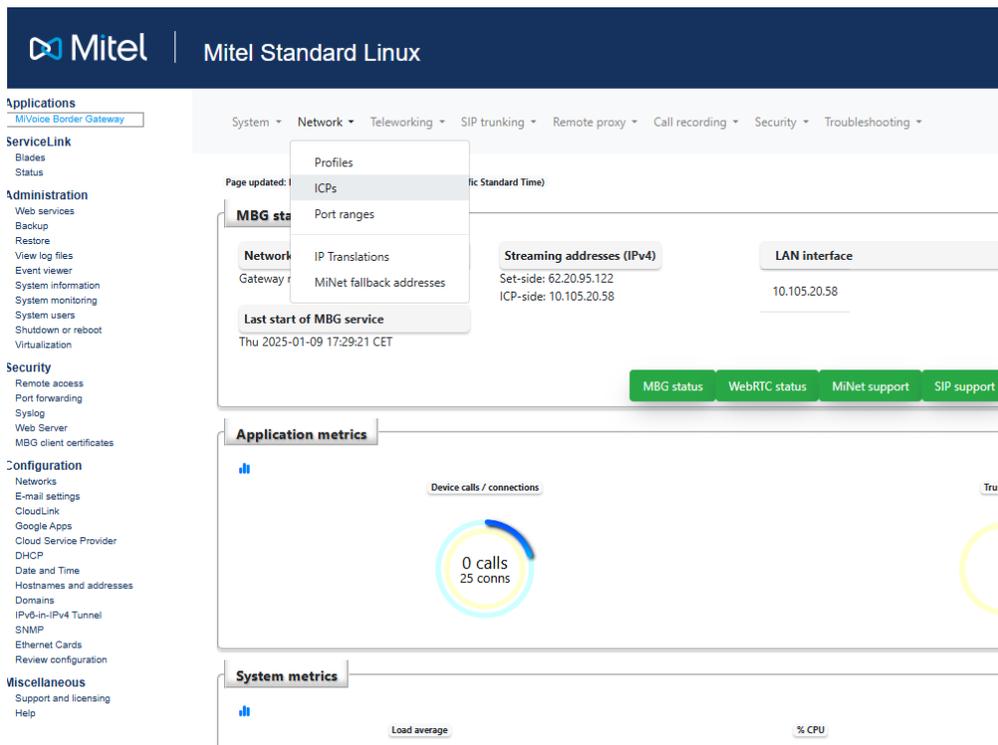
To have the WebRTC calls to work you need access to:

- MBG server
- MXONE Server
- Optionally: Test Client / MBG inbuilt test client

# MBG SERVER CONFIGURATION

The screenshots and examples below is showing MBG 12.x. If you are configuring a different version your interface might look slightly different.

1. The first thing we need to do is to create an ICP. From the top menu, select “Network->ICPs”.



2. On the ICPs page, click the “+” icon to add a new ICP.

The screenshot shows the Mitel Standard Linux web interface. The top navigation bar includes the Mitel logo and the text "Mitel Standard Linux". Below this, there are several tabs: "System", "Network", "Teleworking", "SIP trunking", "Remote proxy", "Call recording", and "Troubleshooting". The left sidebar contains a menu with categories: "Applications" (with "MiVoice Border Gateway" selected), "ServiceLink", "Administration" (with sub-items like "Web services", "Backup", "Restore", "View log files", "Event viewer", "System information", "System monitoring", "System users", "Shutdown or reboot", "Virtualization"), "Security" (with sub-items like "Remote access", "Port forwarding", "Syslog", "Web Server", "MBG client certificates"), "Configuration" (with sub-items like "Networks", "E-mail settings", "Google Apps", "Cloud Service Provider", "DHCP", "Date and Time", "Hostnames and addresses", "Domains", "IPv6-in-IPv4 Tunnel", "SNMP", "Ethernet Cards", "Review configuration"), and "Miscellaneous" (with sub-items like "Support and licensing", "Help").

The main content area displays "Page updated: Tue Aug 16 2022 11:45:20 GMT-0700 (Pacific Daylight Time)" and a note: "To test connectivity to your configured ICPs, or to run a DNS resolution test on configured hostnames, see the [Diagnostics](#) page." Below this is a section titled "ICP Information" containing a table with a "+" icon in the top-left corner, indicating an option to add a new entry.

Default for MiNet	Default for SIP	Name	Hostname or IP address	Type	Installer password
-------------------	-----------------	------	------------------------	------	--------------------

At the bottom of the page, the following text is visible: "MiVoice Border Gateway 11.3.0.49", "Copyright 1999-2022 Mitel Corporation", and "All rights reserved."

- On “Manage ICP” page, enter a name which can be anything you want. For the “Type” field, select “MiVoice MX\_ONE”. For the “SIP capabilities” field, select “UDP, TCP, TLS”. For the “Hostname or IP address” field, enter the MXONE IP address. Click the “Save” button.

Mitel Standard Linux

admin@mbg01-se.mitel.com

Applications

MiVoice Border Gateway

System Network Teleworking SIP trunking Remote proxy Call recording Security Troubleshooting

ServiceLink

Blades

Status

Administration

Web services

Backup

Restore

View log files

Event viewer

System information

System monitoring

System users

Shutdown or reboot

Virtualization

Security

Remote access

Port forwarding

Syslog

Web Server

MBG client certificates

Configuration

Networks

E-mail settings

CloudLink

Google Apps

Cloud Service Provider

DHCP

Date and Time

Hostnames and addresses

Domains

IPv6-in-IPv4 Tunnel

SNMP

Ethernet Cards

Review configuration

Page updated: Mon Jan 20 2025 13:24:07 GMT-0800 (Pacific Standard Time)

The following is a form for modifying an icp entry. You may edit this information as you wish, and click on the "Save" button below when you are done.

**Manage ICP**

Name: mx-one

Type: MiVoice MX-ONE

SIP capabilities: UDP, TCP

Hostname or IP address: 10.105.20.11

MiVoice MX-ONE support

Link to this ICP?

XML listen port: 22223

XML destination port: 22223

Configuration server listen port: 4431

Configuration server destination port: 443

Configuration server address:

Enable

TLS?

TLS?

TLS?

TLS?

Save

- Now we need to add a SIP teleworker user that will be making WebRTC calls. We have to program this user in MBG and in MXONE. From the top menu, select “Teleworking->Manage”.

Mitel Standard Linux

admin@mbg01

Applications

MiVoice Border Gateway

System Network Teleworking SIP trunking Remote proxy Call recording Security Troubleshooting

ServiceLink

Blades

Status

Administration

Web services

Backup

Restore

View log files

Event viewer

System information

System monitoring

System users

Shutdown or reboot

Virtualization

Security

Remote access

Port forwarding

Syslog

Web Server

MBG client certificates

Configuration

Networks

E-mail settings

CloudLink

Google Apps

Cloud Service Provider

DHCP

Date and Time

Hostnames and addresses

Domains

IPv6-in-IPv4 Tunnel

SNMP

Ethernet Cards

Review configuration

Page updated: Mon Jan 20 2025 13:24:07 GMT-0800 (Pacific Standard Time)

The following is a form for modifying an icp entry. You may edit this information as you wish, and click on the "Save" button below when you are done.

**Manage ICP**

Name: mx-one

Type: MiVoice MX-ONE

SIP capabilities: UDP, TCP

Hostname or IP address: 10.105.20.11

MiVoice MX-ONE support

Link to this ICP?

XML listen port: 22223

XML destination port: 22223

Enable

TLS?

TLS?

TLS?

5. In the “SIP profiles and Devices” section, click on the “+” icon to add a new teleworking user.
6. In the “Manage SIP profile” page, check the “Enable” checkbox. For both “Set-side username” and “Icp-side username” fields, use the extension we plan to use as the UC Endpoint user in MXONE. For the “Configured ICP” dropdown, select the MXONE we just created at step 3 above. For both set-side and icp-side passwords, use the SIP password same as the extension number. Click the “Save” button.

**Manage SIP profile**

**Profile**

Enabled

Description 20008 - Bo Stenlund

**Connection**

Configured ICP mx-one

Cluster zone Default

**Set-side Authentication**

Username 20008

Password [Change password](#)

Confirm

**ICP-side Authentication**

Username 20008

Password [Change password](#)

Confirm

**Warning!** Weak SIP passwords have been permitted on this system, but they are never recommended. If you ignore a weak password warning, this account will likely be compromised, resulting in toll fraud.

**Protocol**

PRACK support Enabled

Options keepalives Always

Heartbeat interval 180

Challenge methods Use primary setting [Override](#)

**Media**

Local streaming between device calls Use global setting

Bypass streaming between device calls Use global setting

Codec support Use global setting

**Tone Injection**

Enable

**Set-side RTP security**

Inbound RTP only

Outbound AVP+crypto

Preferred cipher Use global setting

**ICP-side RTP security**

Inbound Use global setting

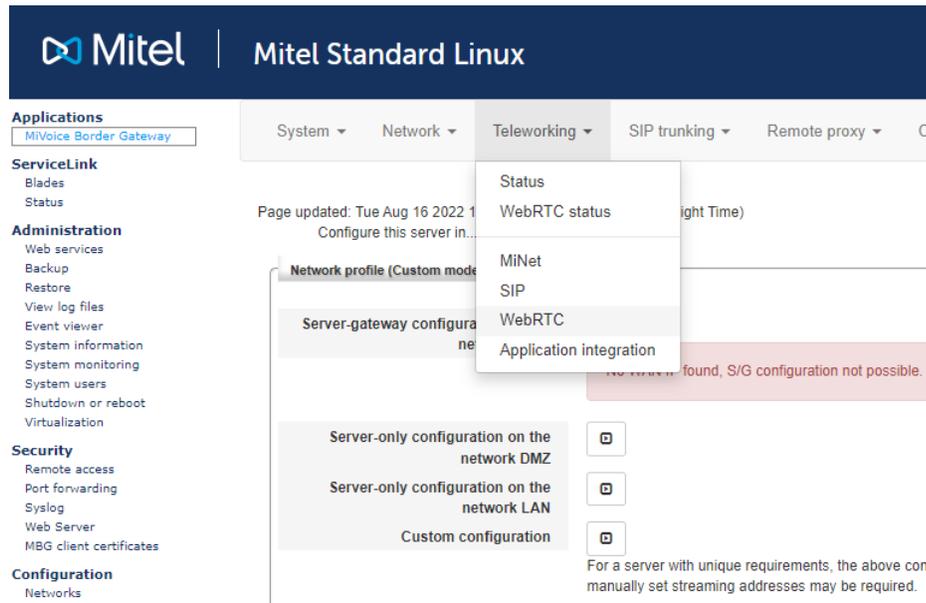
Outbound Use global setting

Preferred cipher Use global setting

MBG may not allow you to add weak passwords, in that case go to System → Settings → Find “Permit weak SIP passwords” in the very bottom of the page and enable the checkbox.

7. If not already done, we need to configure a Network Profile before we can use the MBG for WebRTC. From the top menu, select “Network->Profiles” and click on the right-arrow on the right of “Custom Configuration”, enter the MBG IP address for both “RTP ICP-side override addresses” and “RTP Set-side override addresses” and click the “Apply” button.

Now we need to configure WebRTC, from the top menu, select “Teleworking->WebRTC”. (only needed on MBG versions 11.5 or older):



8. In “WebRTC” page, click the “Enabled” checkbox.
  - a. For the “Hosting mode” dropdown, select “Host WebRTC client locally”.
  - b. For “Webserver shared secret” field, just enter something, it is not used but something must be entered.
  - c. For the “WebRTC protocol security mode” field, just select “Public and Private”.
  - d. “Video enabled” should be unchecked.
  - e. For the “Mode” field, select “Anonymous and Subscriber”.
  - f. Anonymous WebRTC ICP - Select the Configured ICP name
  - g. WebRTC whitelist/blacklist mode - choose “neither”

- Now we need to enable SIP option. From the top menu, select “System->Settings”, in the “SIP options” section, enable UDP, TCP and TCP/TLC protocols.  
If MBG 11.6 or newer is used then enter 192.168.0.1 as ‘Allowed URI names’.

### SIP options

**SIP support**

Protocols: UDP  Private

This is not a secure transport

TCP  Public

This is not a secure transport

TCP/TLS  Public

Certificate: Mitel [Export root cert](#)

**Set-side RTP security**

**Inbound**

SRTP only Accept either SRTP or RTP inbound to this server

SRTP or RTP

RTP only

**Outbound**

SRTP only Send only RTP (plaintext) outbound from this server

AVP+crypto

RTP only

Preferred cipher: AES\_CM\_128\_HMAC\_SHA1\_32

**ICP-side RTP security**

**Inbound**

SRTP only Accept only RTP (plaintext) inbound to this server

SRTP or RTP

RTP only

**Outbound**

SRTP only Send only RTP (plaintext) outbound from this server

AVP+crypto

RTP only

Preferred cipher: AES\_CM\_128\_HMAC\_SHA1\_32

**Set-side Authentication Methods**

SHA-512-256  
SHA-256  
MD5

**Tone Injection**

Enable

Device -- device local streaming

Device -- device bypass streaming

Device -- trunk local streaming

Codec support: Unrestricted

**PRACK support**

Send options keepalives: Only behind NAT

Options interval: 20

Challenge methods: Invite  
Subscribe  
Refer  
Prack

KPML username:

KPML password:

Confirm KPML password:

**WebRTC support**

WebRTC mode: Both

[Change WebRTC passphrase](#)

**Registration Mode** Gap

Set-side registration expiry time: 240

ICP-side registration expiry time: 900

Allowed URI names: + 10.105.20.11  
10.105.20.12

**SIP adaptation support**

SIP adaptation receive pipeline: .....

SIP adaptation send pipeline: .....

**Restrict SIP profiles**

Permit weak SIP passwords

**Warning!** Allowing weak SIP passwords compromises the security of this entire solution. If this server is facing the Internet, then it is highly likely that someone will manage to break into an account with a weak

10. Now we can to start MBG service if not already running. From the top menu, select “System->Dashboard” to see running services, and manage them..

The screenshot displays two main sections of a dashboard. The top section, titled "MBG status", contains several data points and control buttons. It shows the network profile as "Custom mode", the last start of MBG service on "Thu 2024-08-15 18:36:33 EDT", and streaming addresses for Set-side and ICP-side both at "10.70.128.232". The LAN interface is listed as "10.70.128.232". Below this information are five green buttons: "MBG status", "WebRTC status", "MiNet support", "SIP support", and "Call recording support". The bottom section, titled "Application metrics", features a bar chart icon and three circular gauges. The first gauge, "Device calls / connections", shows "0 calls" and "0 conns". The second gauge, "Trunk calls", shows "0". The third gauge, "Active taps", shows "0".

Network profile	Streaming addresses (IPv4)	LAN interface	WAN interface	Third interface
Custom mode	Set-side: 10.70.128.232 ICP-side: 10.70.128.232	10.70.128.232	---	---

**Last start of MBG service**  
Thu 2024-08-15 18:36:33 EDT

MBG status | WebRTC status | MiNet support | SIP support | Call recording support

Device calls / connections	Trunk calls	Active taps
0 calls 0 conns	0	0

## MX-ONE CONFIGURATION

### SIP EXTENSION PASSWORD

For the Registration of any extension to on MBG → WebRTC Gateway the MBG does not accept Register of users without challenging SIP password.

Which means SIP Passwords must be added for extensions on MX-ONE side with MD5 Encryption. The auth code must be set to the extension number in order to used by Web Agent with WebRTC.

On MX-ONE side set the passwords for the extensions by the below commands:

1. `auth_code -i --d <extension> --auth-code <extension> --csp 0 --cil <extension> \ --hash-type md5a1`
2. `auth_code -p -d <extension>`

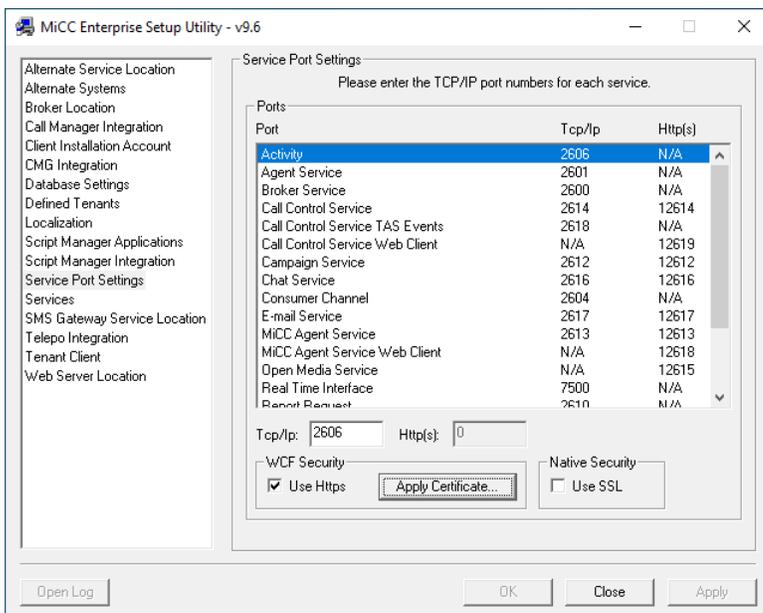
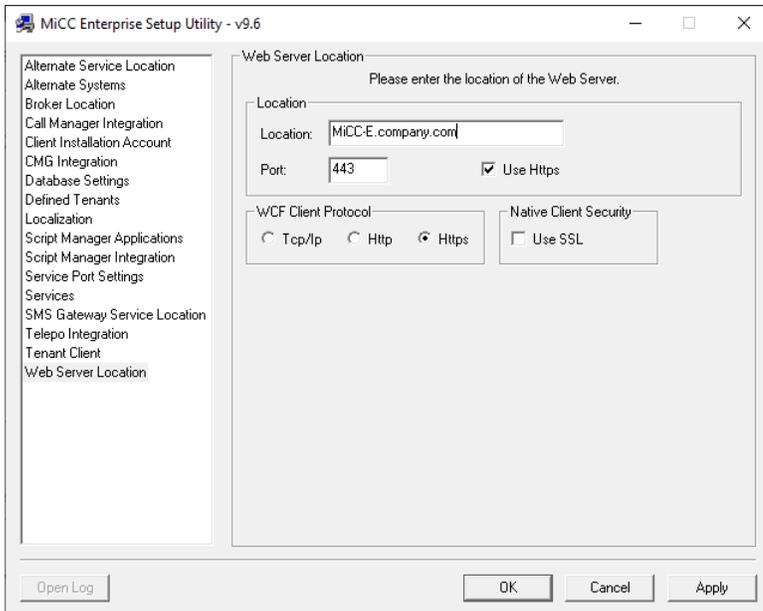
Example:

```
auth_code -i --d 5291 --auth-code 5291 --csp 0 --cil 5291 --hash-type md5a1
auth_code -p --d 5291
```

```
customer dir  auth code                               cil code CSP restr new customer
=====  =====
      0 5291 md5a1:3417465e46c5d2b3fb78d0e8489bb278      5291 0      -
```

## CONFIGURE THE MICC ENTERPRISE SERVER

The MiCC Enterprise system must be configured to use HTTPS in order for WebRTC to work. This is configured using the MiCC Enterprise Setup Utility.



The location and domain of the MBG server needs to be configured on the MiCC-E server. Open the config.json file located in the *<MiCC-E install location>\Services\Web\WebAgent\assets* folder in a text editor and change the “webSocketServerURL” and “domain” entries in the “webRTCConfig” section to point to the location of the MBG server.

Example:

```
"webRTCConfig": {  
  
    "userAgent": "Mitel-UC-Endpoint",  
  
    "webSocketServerURL": "wss://vm-mbg11-6.seclab.com:5063",  
  
    "domain": "vm-mbg11-6.seclab.com"  
  
}
```

**Note:** If MBG 11.5 or older is used then leave the 192.168.0.1 entry for the “domain” parameter.

If the majority of Web Agent users will be using WebRTC then the default value for the Extension Type input field in the Logon dialog can be set in the config.json file by setting the *defaultExtensionType:softPhone* parameter to *true*.

## CONFIGURE THE WEB AGENT CLIENT

### 1. DNS

Each client device needs to be able to reach the MBG server, so if the MBG is reached by server name or FQDN the DNS must be able to resolve them. If not, entries will have to be added to the clients HOSTS file. Same things would apply for the resolving the MiCC-E server name.

### 2. Certificates

- a. Login into MBG server, Go to Security → Web Server menu
- b. Under “Web Server Certificate” tab, find “Download the current web server certificate” and click on Perform button, it will download the certificate
- c. Use the Certificate Manager in Windows to install the certificate into the “Trusted Root Certification Authorities”.

## VALIDATE THE CONFIGURATION

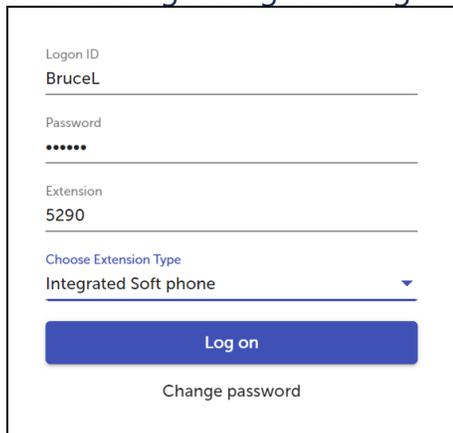
The configuration can be validated in two ways.

### 1. Using Web Agent

If the MiCC Enterprise system is already in place and is configured, then the MBG setup can be validated using Web Agent. Start Web Agent in a Chrome browser by loading:

*http://<MiCC Enterprise Server>/WebAgent*  
 or in case of a multi-tenanted system loading:  
*http://<MiCC Enterprise Server>/WebAgent/#/login/<Tenant Name>*

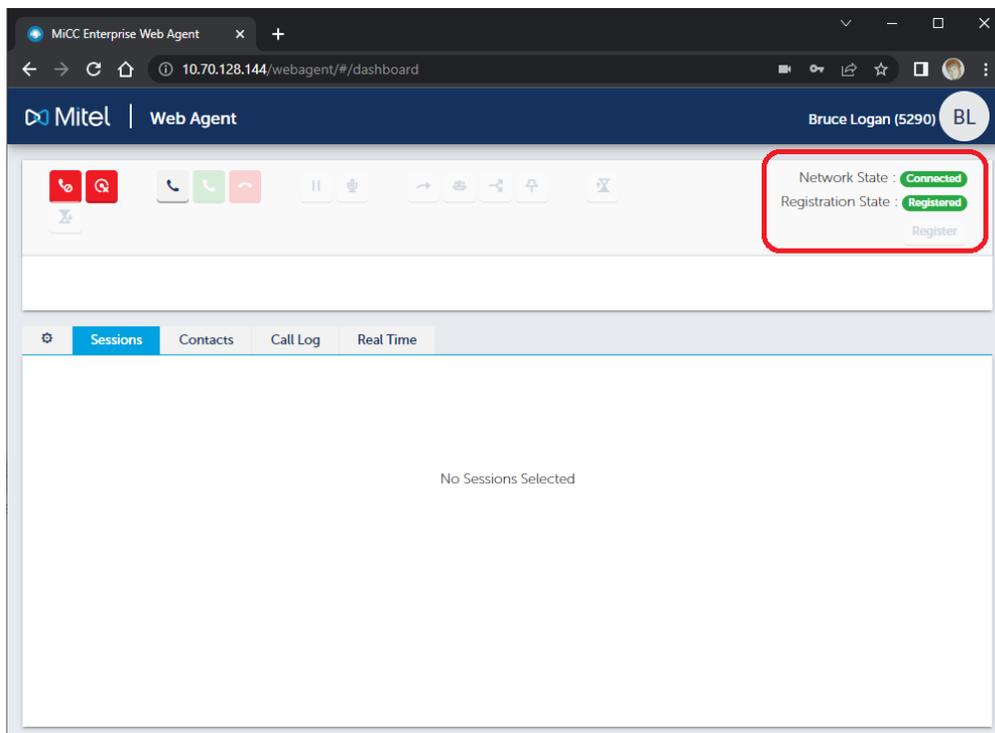
The Web Agent logon dialog will be presented:



The logon dialog form contains the following fields and elements:

- Logon ID: BruceL
- Password: masked with six dots
- Extension: 5290
- Choose Extension Type: Integrated Soft phone (dropdown menu)
- Log on button (blue)
- Change password link

Enter the SIP extension number that has been configured in MX-ONE and MBG and select *Integrated Soft Phone*. If all goes well then Web Agent will load, and Network State and Registration State should be shown as green:



If not, then click F12 to enter Console mode in Chrome to troubleshoot connectivity and Registration issues.

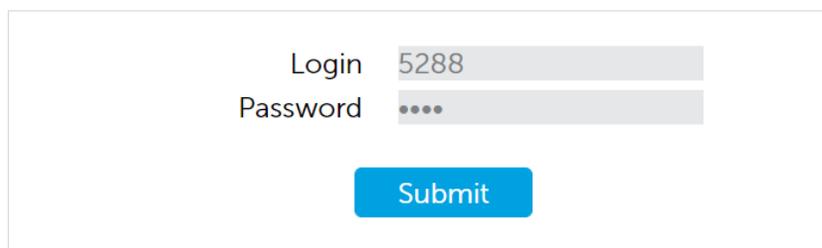
2. Using MBG inbuilt app (MBG 11.5 or older)

To use the MBG built-in test app, from the top menu of the MBG server manager, select "Teleworking->WebRTC", and click the "?" icon. This will bring up the help page.

As per the help page, there are two different ways to launch the client app. One is Anonymous call mode (c://<MBG-FQDN>/webrtc/call.php?to=<CalledNumber | SipUri>) and the other is the Subscriber call mode (<https://<MBG-FQDN>/webrtc/index.php>) Subscriber call mode will be used in this example.

Note that you might have to add the <MBG-FQDN> in your computer's hosts file (c:\Windows\System32\drivers\etc\hosts) if it is not in your corporate DNS.

When you enter the URL in your browser, you will be prompted to enter Login/Password. The Login is the extension number and the password is the SIP password for the extension.

A login form with two input fields. The first field is labeled "Login" and contains the text "5288". The second field is labeled "Password" and contains four dots. Below the fields is a blue "Submit" button.

Note that the password needs to be the MD5 hashed password as entered above for the SIP user.

If correct credential is entered, you will see this and you can make WebRTC call by enter a number in the "Name/Number" field.

